NRC Security Operations Center
A Small(er) Agency SOC Perspective

Liz Chew / Mario Gareri
U.S. Nuclear Regulatory Commission
Office of Information Services
IT Operational Security Team

GFIRST – August 17, 2010

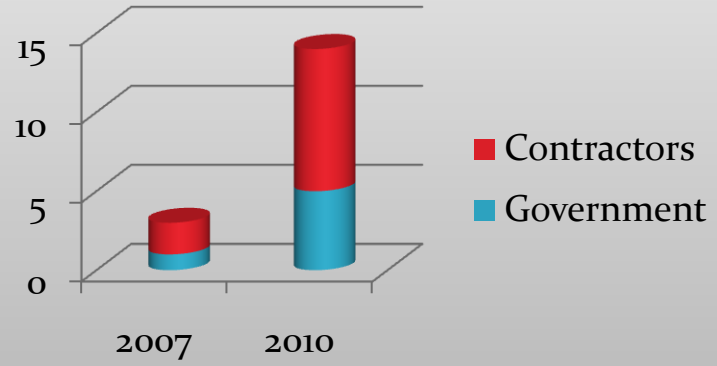
IT Security Operations at the NRC

Agenda

- Overview - NRC IT Security Operations
- Small(er) Agency IT Security Challenges
- Notable Network Threats
- Security Operations Strategies
- Incident Prevention Strategies
- NRC SOC Tools
- Threat Detection Methods
- Case Study - Malware

Overview - NRC IT Security Operations

- US Nuclear Regulatory Commission oversees civilian use of nuclear materials and facilities
- 5,000 users + 8,000 endpoints distributed over 70 locations
- Internet access for all locations is provided through NRC HQ located in Rockville, MD
- NRC SOC Personnel:
  - 2007 - 1 Fed, 2 contractors
  - 2010 – 5 Feds, 9 contractors



Overview - NRC IT Security Operations

NRC SOC Primary Functions
Management of Information Security Systems
Monitoring of NRC IT Environment
Investigation of Potential Incidents
Incident Response
Analysis of Emerging Threats
IT Security Project Support

Overview -NRC IT Security Operations

NRC SOC Structure

Security Management

- Administer firewalls, proxy servers, mail gateways, SSL VPN, NAC, VA Scanners, DNS, logging appliances

Security Analysis

- Administer IDS/SIEM, conduct networking monitoring and incident investigation

Teams are co-located to promote information sharing and situational awareness

Small(er) Agency IT Security Challenges

Business Operational Needs vs. Security Measures

Funding for network security technologies and staff

OMB/FISMA compliance requirements

Staying aware of new Internet threats

Business operational needs

Finding the right people with the right skills, cross training

Notable Network Threats

- The delivery of malicious software during routine web browsing, usually through drive-by downloads
- Spear Phishing
- The introduction of malicious software through removable media
- Direct reconnaissance for vulnerabilities and attempted exploits of public facing NRC systems

Notable Network Threats

Meeting the Challenges

Leverage automated threat prevention and detection tools to their full capability

Supplement the use of automated detection with analytical threat detection methods

Recognize that no single security technology alone or in combination provides perfect protection against the wide array of Internet threats

Security Operations Strategies

Prevention	Detection	Response
• Proactive measures to protect the NRC IT environment	• Automated and manual methods for detecting internal and external threats	• Processes for responding to all IT security incidents

Incident Prevention Strategies

- No direct access from desktops to Internet, all user traffic must be proxied
- Automated systems provide web & E-mail content filtering/AV scanning at perimeter and at desktops
- Block malicious domains & IP addresses on firewall & proxy server based on publicly available data
- The .ru and .cn TLD's are blocked on proxy servers, also no access to "Social Networking" sites
- Block spear-phishing senders on mail gateways - email addresses of spear phishers blocked as they are discovered through SOC analysis and data sharing on US-CERT Mercury Portal

Incident Prevention Strategies

Preventive Security Statistics

Mail Security Gateways

- Each month, an average of:
- 4 million emails blocked by reputation filtering (~80% of total inbound messages)
- 50 messages with viruses blocked by mail gateways

Anti Virus

- Each month, an average of:
- 180 viruses blocked by web antivirus scanners
- 100 viruses blocked by desktop antivirus

NRC SOC Tools

- NRC boundary and network protection tools/devices defend and protect NRC infrastructure from both internal and external threats
- Network tools are complemented with monitoring and analysis by NRC and contractor security specialists

Firewalls
Mail Security Gateways Spam filtering and email anti-virus scanning
Proxy Server / Reporter Content filtering for web traffic
Web Anti-Virus Scanner Operates in conjunction with proxy server to scan all web content for malicious software
Vulnerability Scanner

NRC SOC Tools

Vulnerability Assessment Scanner / Compliance Manager Reporting Platform for aggregation, reporting, and analysis of data for all network devices that profiles their applications, services, vulnerabilities, and compliance status
Intrusion Detection System (IDS) Sensors
Network Access Control (NAC) System
Log Management Appliances
Security Information and Event Management (SIEM) Appliance
Desktop antivirus and malware detection
SSL VPN/ Remote Access Gateway Provides secure remote access to Citrix desktop and SSL VPN access

Threat Detection Methods
Automated Daily Reports Review

Automated reports provide daily summaries of significant information from ~15GB of security log data. Example reports include:

Proxy Server
Top Surfers, Top Blocked Users, Spyware-infected hosts

Firewall
Denied outbound connections

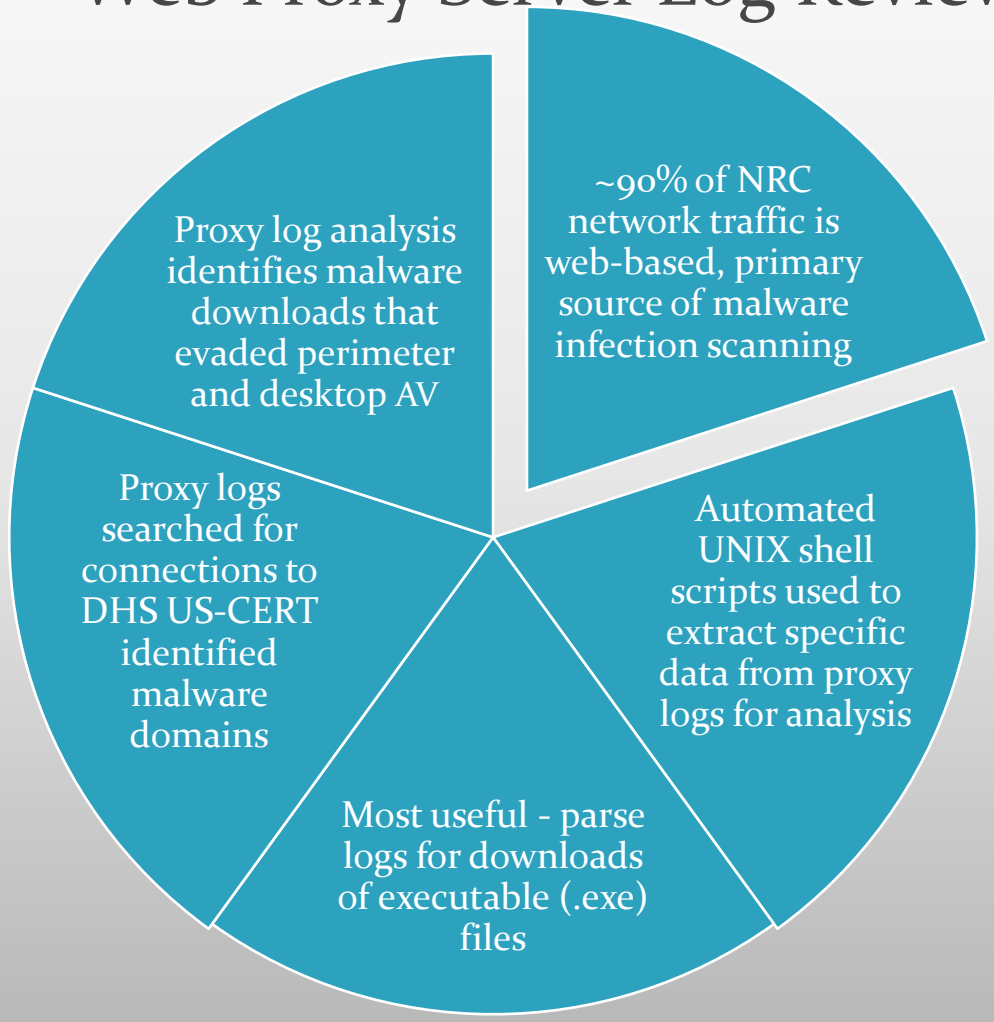
Web AV Scanner
Blocked virus download summary

Mail Gateway
Blocked email virus summary

VA Scanner
Hosts with highest vulnerability scores

Threat Detection Methods

Web Proxy Server Log Review



Threat Detection Methods

SIEM Monitoring

SIEM appliance correlates log information from firewalls, IDS, and other security devices

Provides real-time alerts for detection of patterns of suspicious activity that would not be evident by analysis of any one log source

Example: Alerts sent for a host that triggered IDS alerts, had blocked malware downloads, multiple firewall denies, or suspicious traffic based on netflow analysis

Threat Detection Methods
AV Console Monitoring

AV provides real-time alerting of Windows workstation/server infections

- SOC investigates when AV detects but does not successfully quarantine/clean virus infection
- Help Desk ticket is opened for further action if needed (e.g. reimaging hard drive)
- Reporting features allow for trend analysis and identification of malware outbreaks

Threat Detection Methods
Publicly Available Tools

Malicious Domain / IP Address Lists

- ddanchev.blogspot.com
- malwaredomainlist.com

Online Website Analysis Tools

- web-sniffer.net
- wepawet.iseclab.org

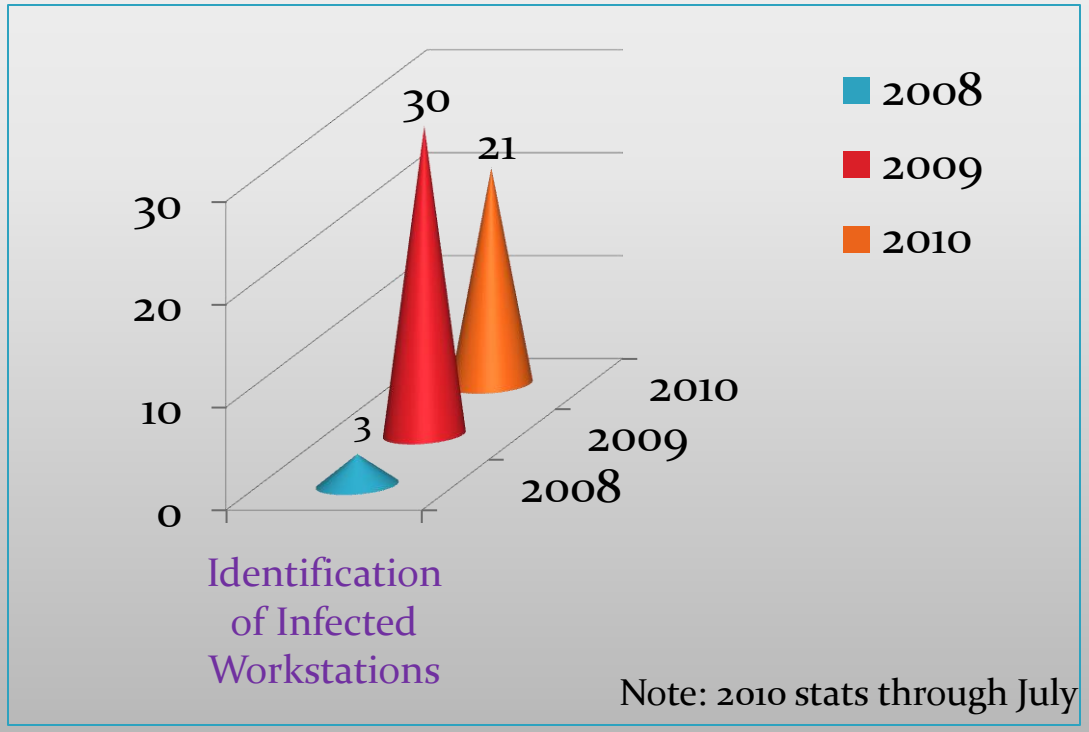
Suspicious File Analysis Tools

- virustotal.com
- anubis.iseclab.org
- Malzilla by Bobby

Threat Detection Methods

Detective Security Statistics

Large annual increase is primarily due to improved surveillance and detection, including automated search of security logs and review of log extracts and reports by skilled analysts

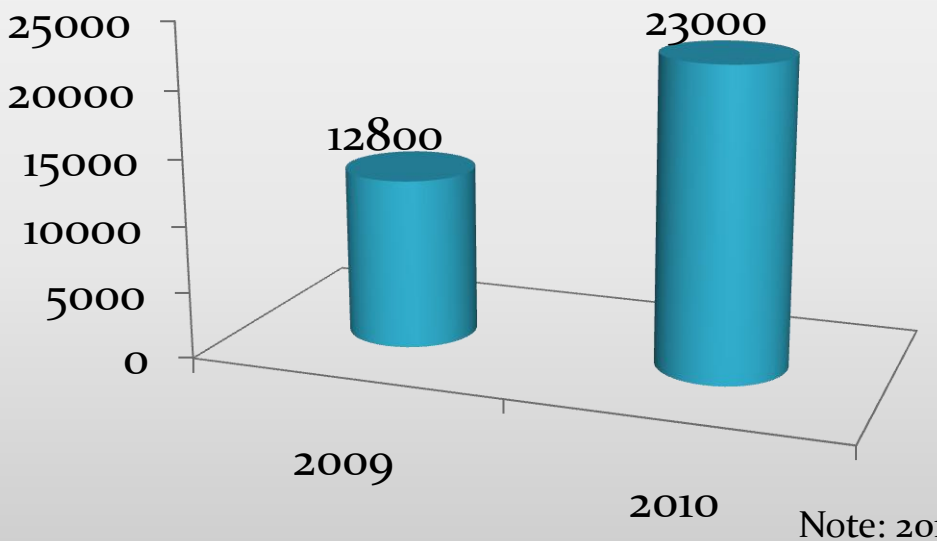


Note: 2010 stats through July

Threat Detection Methods

Security Response Statistics

Blocking Malicious Sites



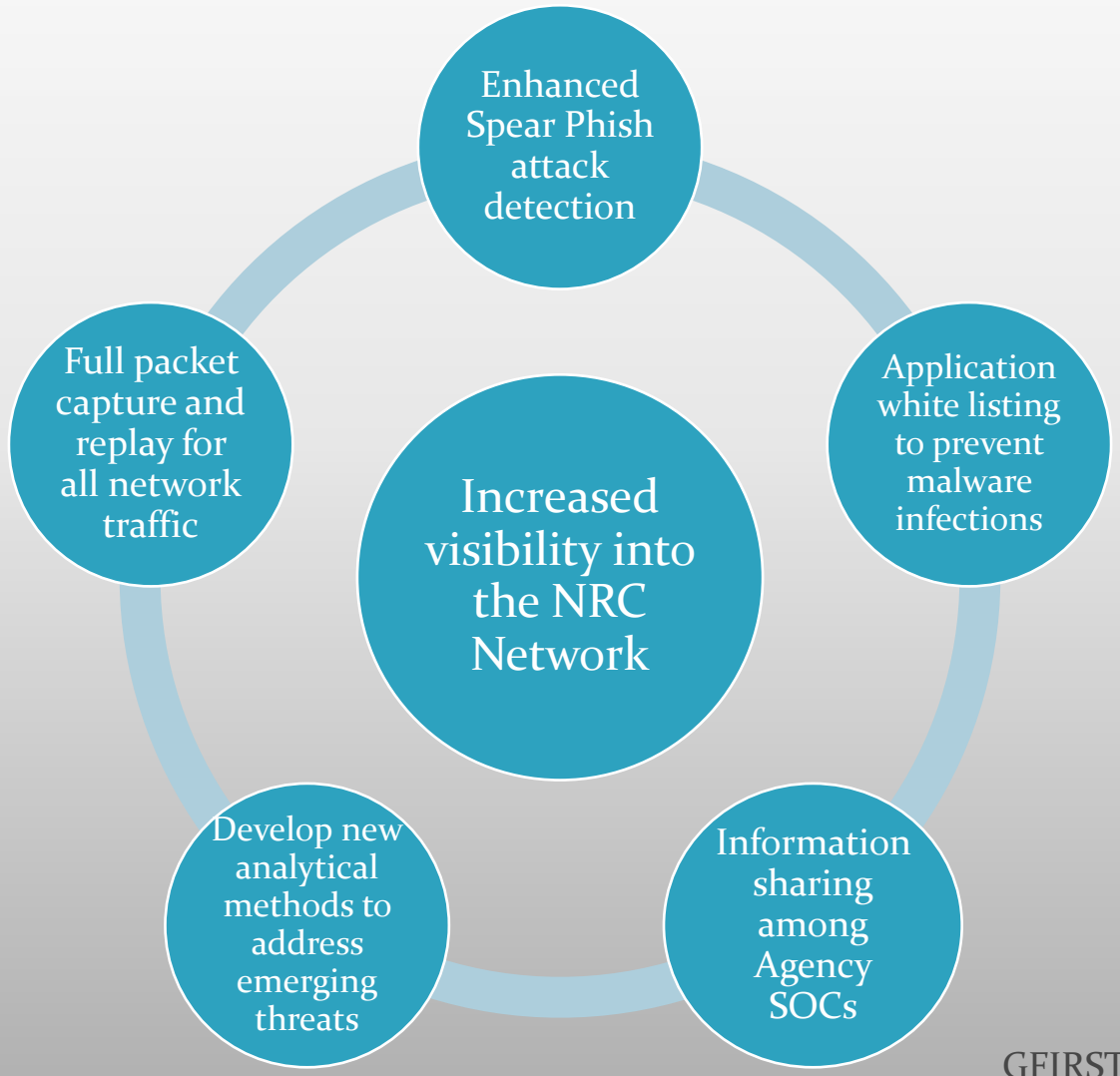
Note: 2010 stats through July

Information from US-CERT and reputable Internet network security sources is used to populate block lists on the firewall and proxy servers.

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Threat Detection Methods

Desired Improvements



Case Study – Malware
Detection

Incident from June 2010 exemplifies strengths of NRC SOC approach:

- Use security technologies from leading vendors
- Augment tools with publicly available network intelligence
- Review security logs to identify source of threat
- Collaboration between SOC Security Analysis and Security Management teams to prevent additional malware infections

Case Study – Malware

SIEM Enhancement through Publicly Available Data

- SIEM tool customized to download the content from malwaredomainlist.com and extract unique IP addresses each day.
  - Malwaredomainlist.com is a website that lists malicious domains and IP's and is updated frequently.
- Malicious IPs from the site are added to a "Malware" rule group in SIEM tool, which alerts on any event that is sourced or destined to an IP address in the "Malware" group.

Case Study – Malware
Detection

Incident Overview

SIEM detected an NRC workstation beaconing out to a known malicious IP that was posted on malwaredomainlist.com

SIEM event description

Offense #3182

Start Time: Tue Jun 08 14:32:07 EDT 2010

Description: Malware - External - Communication with BOT Control Channel preceded by Multiple Vector Attacker Detected

Event Count: 42 events in 4 categories

Case Study – Malware
Analysis

Log Analysis:

Review of proxy server logs from workstation IP address identified the malicious URL hxxp://10[.]arsdh[.]in/x/1.php as the source of infection

A file with 98,695 bytes was downloaded

Proxy log entry:

Message: 2010-06-08 "[08/Jun/2010:14:32:23 -0400]" 1344 10.10.10.55 200 TCP_NC_MISS 98,695 338 GET hxxp 10.arsdh.in 80 /x/l[.]php ?s=midi& - - DIRECT 10.arsdh.in application/octet-stream

Case Study – Malware Analysis

Client makes HTTP GET request for 1.php file, server responds with file called svchost.exe

Client request

Client requests php file from server :
hxxp://10[.]arsdh[.]in/x/1.php ?s=midi&" accepted

Server response

HTTP/1.1 200 OK
Server: nginx/0.6.39
Date: Tue, 08 Jun 2010 20:06:30 GMT
Content-Type: application/octet-stream
Content-Disposition: inline; filename=svchost.exe.

Client result

When the client is redirected maliciously and requests the file "1.php", the malicious server responds with the HTTP tag: "content-disposition: inline filename" to change the filename from "1.php" to "svchost.exe" upon download.

Case Study – Malware
Analysis

After installation of the svchost.exe malware, the infected machine starts to beacon out to the domain hxxp://liii16bo[.]com on port 443.

Log message:

06/08/1014:32:24 Message: 351 10.10.10.5 403 TCP_DENIED 185 145 CONNECT **tcp liii16bo.com 443** / - - - NONE - - - DENIED "Suspicious" - - 10.10.10.51 SG-HTTP-Service

Case Study – Malware
Analysis

Use of publicly available tools

The malicious executable is submitted to virustotal.com where it is found to have a low detection rate (~5%)

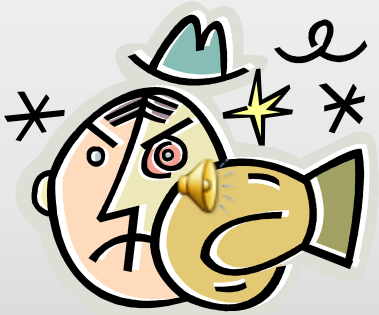
File **svchost.exe** received on **2010.06.08 20:07:45 (UTC)**
Current status: **finished**
Result: **2/41 (4.88%)**

Panda	10.0.2.7	2010.06.08	Suspicious file
PCTools	7.0.3.5	2010.06.08	-
Prevx	3.0	2010.06.08	Medium Risk Malware

Case Study – Malware
Final Actions/Summary

- NRC user became infected by browsing the web through malicious redirect and drive-by download
- Malware detected by a combination of publicly available tools/websites, security devices, and SIEM tool
- Proxy servers and logs played a vital role in piecing together the series of events
- All malicious websites involved were blocked on the firewall and proxy servers
- Infected workstation was re-imaged

Questions?



NRC SOC Rocks!